UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Jacqueline Mekhail, individually, and on behalf of those similarly situated, Plaintiff, v. North Memorial Health Care, d/b/a North Memorial Health, Defendant.	Case No. 0:23-cv-00440-KMM-TNL **AMENDED CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiff Jacqueline Mekhail ("Plaintiff"), on behalf of herself and all others similarly situated, by and through her attorneys of record, asserts the following against Defendant, North Memorial Health ("North Memorial" or "Defendant") based upon personal knowledge and upon information and belief, and the investigation of counsel, which included, among other things, consultation with experts in the field of data privacy.

INTRODUCTION

1. Plaintiff brings this class action complaint on behalf of a class of persons impacted by Defendant's unauthorized disclosure of their highly sensitive Personal Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively "Sensitive Information") to third parties. Defendant solicited and obtained Plaintiff's and the Class's Sensitive Information as part of its ordinary business activities as a medical services provider.

2. Defendant provides patients with an online website, www.northmemorial.com, to *inter alia*, research information about medical issues and

conditions, research doctors, and provide a patient portal, which is available at (https://northmemorial.com/mychart-medical-records/)

3. Defendant's "patient portal" (https://northmemorial.com/mychart-medical-records/) further allows patients to check in and schedule appointments online, do E-Visits, communicate with their healthcare providers, review test results, pay a medical bill or sign up for a payment plan, receive paperless billing statements, get a cost estimate, request prescription refills, among other sensitive and private communications.

4. Defendant encourages its patients to use its website, www.northmemorial.com, and online patient portal, https://northmemorial.com/mychart-medical-records/, (collectively "Websites") to communicate with their medical providers, schedule appointments and review test results. And in doing so, Defendant represents to patients that its online patient portal is both a secure platform, and the information provided therein will remain secure and confidential. North Memorial fails to disclose or omits the fact that it shares patient's online activities and personal health information with Meta Platform, Inc. ("Meta") via the Meta Pixel ("Pixel").

5. Recently, Plaintiff became aware that Defendant incorporates Meta tracking technology, the Pixel, on the North Memorial Websites. Pixel is a snippet of code that, when embedded on a third-party website, tracks the website visitor's activity on that website and sends that data to Meta. This includes tracking and logging pages and subpages the website user visits during a website session which reveal patient status and other personal identifying and protected healthcare information, clicks, searches and other submissions to the website, which in many cases includes sensitive personal, and

identifying information that is not anonymized. Indeed, Pixel is routinely used to target specific customers by utilizing the data gathered through the pixel to build profiles for the purpose of future targeting and marketing. Here, the information transmitted to third-party Meta, without Plaintiff's consent, most certainly included private healthcare information, which is some of the most personal and sensitive data Plaintiff has.

6. Additionally, when a patient communicates with North Memorial's Websites where the Pixel is present, the Pixel source code causes the exact content of the patients' communications with the Websites to be re-directed to Meta in a fashion that identifies them as a patient. For example, Plaintiff Mekhail was a patient of North Memorial and in the course of receiving medical care at North Memorial used the Websites to communicate with her providers and conduct other medical related research. Unbeknownst to Plaintiff, and other patients, when she accessed the portal to sign in, the Pixel secretly deployed on the Websites sent the fact that she was attempting to login to the patient portal to Meta.

7. Defendant's use of Pixel allowed for a broad scope of patient information, including highly confidential medical information, to be collected and transmitted to Meta without patients' knowledge or consent. Specifically, Pixel is designed to track website users' activity on a website or application. It can capture how visitors interact with the site, including buttons they click and information they provide to form fields or otherwise. These are collectively known as "Website Communications."

8. Defendant used Pixel to improve and save costs on its marketing campaigns, improve its data analytics to increase revenue by, among other things, attracting new

patients and improving its services for existing patients. Defendant also used Pixel to gain insight into patients, through secret tracking, that it could not otherwise have or use.

9. As a result of Defendant's use of Pixel, Plaintiff's and the Class's Sensitive Information, including computer IP addresses; dates, times, and/or locations of scheduled appointments; information about patients' health care providers; types of treatments or conditions researched; type of appointment or procedure scheduled; communications between patients and others through the online patient portal, which may have included first and last names and medical record numbers; information about whether patients have insurance; gender and sexual orientation; and if a patient had a proxy portal account, the name of the proxy, and other information submitted by Plaintiff and the Class on Defendant's website or application, was compromised and disclosed to third parties without authorization or consent.

10. Such private information would allow Meta to know that a specific patient was seeking confidential medical care or being treated for a specific condition.

11. Plaintiff and the Class never consented to, authorized, or otherwise agreed to allow Defendant to disclose their Sensitive Information to anyone other than those reasonably believed to be part of Defendant, acting in some medical care related capacity. Despite this, Defendant knowingly and intentionally disclosed Plaintiff's and the Class members' Sensitive Information to its vendors and other undisclosed third parties. Plaintiff and the Class Members also did not consent to the Defendant secretly tracking and disclosing their Website Communications and other online user behaviors while on North Memorial's Websites.

12. The exposed Sensitive Information of Plaintiff and the Class members can and will likely be further exposed or disseminated to additional third parties who will utilize that data for retargeting or possibly even insurance companies utilizing the information to set insurance rates.

13. As a direct and proximate result of Defendant's unauthorized exposure of Plaintiff's and the Class's Sensitive Information, Plaintiff and the Class members have suffered injury including an invasion of privacy, loss of the benefit of the bargain Plaintiff and the Class considered at the time they bargained for medical services and agreed to use Defendant's website and the patient portal for services, statutory damages and the continued and ongoing risk to their Sensitive Information.

14. As such, Plaintiff and the Class bring this action to recover for the harm they suffered, and assert the following claims: Violation of Electronic Communications Privacy Act ("ECPA") (18 U.S.C. §§ 2511), Violation of the Minnesota Wiretap Act (Minn. Stat. § 626A.02), Violation of the Minnesota Consumer Fraud Act (Minn. Stat. § 325F.69), Violation of the Minnesota Uniform Deceptive Trade Practices Act ("MUDPTA") (Minn. Stat. § 325D.43-48), Violation of the Minnesota Health Records Act Minn. Stat. §§ 144.291 and 144.293, Invasion of Privacy, and Unjust Enrichment.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interests or costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a

different state from Defendant. This Court further has federal question jurisdiction pursuant to 29 U.S.C. § 1331 because this Complaint asserts claims pursuant to Defendant's violations of 28 U.S.C. § 2511.

16. This Court has jurisdiction over this action because Plaintiff is a resident and citizen of the State of Minnesota who received health care from Defendant while in the State of Minnesota. Defendant is a Minnesota corporation with its principal office located at 3300 North Oakdale Avenue, Robbinsdale, MN 55422.

17. Venue is proper in this Court because Defendant's headquarters are located here, and Plaintiff's claims arise from Defendant's conduct in this County.

PARTIES

18. **Plaintiff** is a natural person domiciled in the State of Minnesota. Her permanent address is located in Woodbury, Minnesota.

19. Plaintiff is a former patient of Defendant and began receiving medical services from Defendant in or around October 2021. Through those services, Plaintiff used Defendant's website and patient portal and provided her Sensitive Information to Defendant, including, without limitation, her name, address, date of birth, medical history, including prescriptions and diagnoses, and medical insurance information. Also, through the services Plaintiff received, Defendant created, maintained, and stored additional PHI for her, including, but without limitation, medical treatment, diagnoses, prescriptions, and insurance information. Plaintiff visited North Memorial's patient portal in connection with medical care she received from North Memorial including to review doctor notes, bills, and medical records.

20. To receive services from Defendant and to use Defendant's Websites, Plaintiff was required to provide personally identifying information, along with other Sensitive Information.[1] Indeed, Defendant's Privacy Policy states that it needs Plaintiff's and the Class members' PII "to understand [their] needs and provide [them] … service."[2] Defendant encouraged and advised Plaintiff to utilize Defendant's online website and patient portal to make appointments, track and receive test results, receive medical treatment, communicate with medical professionals, including doctors, nurses, and other staff, and exchange private, personal, and in most cases confidential information regarding her treatment.

21. Plaintiff is a Facebook user and has had a Facebook account since at least 2009. Plaintiff also maintains an Instagram account.

22. Plaintiff reasonably expected that her online communications with Defendant were between her and Defendant and that such communications would not be shared with third parties without her consent. Without Plaintiff's knowledge, consent, or authorization, Defendant exposed and intentionally allowed third-party Meta to intercept Plaintiff's personal, private, and confidential information through Meta Pixel.

23. After using Defendant's website, it is Plaintiff's recollection that she received some targeted advertisements related to information she had submitted to Defendant via Defendant's Websites.

[1] https://northmemorial.com/privacy-policy/.

[2] *Id.*

24. **Defendant** North Memorial is a Minnesota corporation, is licensed to do business in the State of Minnesota and has its principal business in Robbinsdale, Minnesota. Defendant has approximately 25 specialty and primary care clinics, urgent and emergency care offerings, medical transportation services and two hospitals within the state of Minnesota.[3][4]

25. Plaintiff had her Sensitive Information disclosed by Defendant's breach of her privacy.

FACTUAL BACKGROUND

A. Defendant Collected, Maintained and Stored Sensitive Information

26. Defendant North Memorial started as a single hospital in 1954. Today, Defendant has more than 350 health care providers and more than 6,000 team members.[5]

27. To obtain healthcare services, patients, like Plaintiff and the Class, must provide Defendant with highly sensitive information, including PHI, PII, or both. Defendant compiles, stores, and maintains the highly sensitive PII and PHI and, often, through the provision of its services, creates records containing additionally highly sensitive data concerning patients' medical diagnostics, treatment, and other personal information documented by medical providers. Defendant serves hundreds of thousands of individuals every year, meaning it has created and maintains a massive repository of Sensitive Information.

---

[3] https://northmemorial.com/about-us/.

[4] https://northmemorial.com/visit-a-location/location-search/?zipcode&locationType=primary-care.

[5] https://northmemorial.com/about-us/.

28. Defendant tells patients it will keep their Sensitive Information secure and private. Indeed, Defendant maintains a Privacy Policy through which it states: "North Memorial Health is committed to ensuring that your privacy is protected."[6] The Policy further states that North Memorial "protect[s] health and medical information as required by federal and state privacy laws."[7]

29. Defendant's Notice of Privacy Practices provides that North Memorial required by law to make sure that medical information that identifies you is kept private.[8]

30. Plaintiff and the Class had a reasonable expectation of privacy and relied on Defendant to protect the Sensitive Information provided to it and created by it, especially because, medical facilities are always required to maintain confidentiality of patient records, with very limited exceptions. Defendant knew or should have known that failing to adequately protect patient information could cause substantial harm. Moreover, through its Privacy Policy, Defendant acknowledged its obligation to reasonably safeguard sensitive information against unauthorized disclosure to third parties like Meta.

31. A privacy violation of this type, in which Defendant intentionally granted access to third-party Meta to record and collect information on the company's systems, including within the patient portal, collect user data, including Sensitive Information and highly confidential medical records without restriction, could not occur but for Defendant's

[6] https://northmemorial.com/privacy-policy/.

[7] *Id.*

[8] https://northmemorial.com/wp-content/uploads/2017/03/North-Memorial-Health-notice_of_privacy_practices_2017.pdf.

blatant disregard for patient privacy. Defendant violated several basic privacy and data standards regarding patient privacy and confidentiality.

32. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiff's and the Class's Sensitive Information but rather intentionally and knowingly granted Meta access to confidential information that it knew or should have known was unlawful and divulged highly sensitive information.

33. Consequently, Meta, and potentially other third parties, obtained access to and collected confidential patient data without the patients' authorization, resulting in a significant invasion of patient privacy and breach of sensitive data.

B. Defendant Exposed Its Patients' Sensitive Information

34. Defendant implements Meta's Pixel on its Websites. Pixel tracks website and application users' activity. If a user accesses a website hosting Pixel, Meta's software will secretly direct the user's browser to send a separate message to Meta's servers. This second communication contains the original request the user sent to the host website, in this case Defendant, along with the additional data Pixel is configured to collect. This communication happens concurrently with the first communication the user initiates with the host website.

35. To illustrate this process, consider a patient who opens Defendant's website and clicks on the "Providers" or "Find a Provider" tab. When the user clicks this tab, her browser sends a request to Defendant's server requesting that server load the "Provider" or "Find a Provider" page. Because Defendant utilizes Meta's Pixel, Meta's code

surreptitiously duplicates the communication from the user to Defendant and sends it to Meta's own servers, along with additional information that includes the user's identity.

36. After collecting this information, Meta can process it and add it to their aggregates of consumer data, which may ultimately be used for advertising or other revenue generating schemes.

37. Every time Defendant sends patients' data to Meta, the patients' Sensitive Information is unlawfully disclosed. Defendant could have configured its website and applications to not communicate or share any information with third parties, or to limit the information it communicated to third parties, and maintain the necessary security and confidentiality, but it did not.

38. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Meta: (1) Plaintiff's and the Class Members' status as medical patients, or alternatively, Plaintiff and the Class Members' consideration of becoming a medical patient of Defendant; (2) Plaintiff's and the Class Members' communications with Defendant; (3) Plaintiff's and the Class Members' medical appointments, location of treatments, specific medical providers, and specific medical conditions and treatments; (4) PII including but not limited to patients' locations, an IP address, device identifier, and/or an individual's unique Facebook user number ("FID").

39. Despite the highly sensitive nature of the information Defendant obtained, created, and stored, Defendant inexplicably failed to take appropriate steps to protect the privacy of the PII and PHI of Plaintiff and the Class, and instead intentionally employed Pixel to willingly and intentionally disclose patient data to third-parties including Meta.

40. Defendant deprived Plaintiff and the Class members of their privacy rights when it: (a) implemented Pixel that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and private information; (b) disclosed patients' protected information to Meta—an unauthorized third-party; and (c) failed to provide notice to Plaintiff and the Class members or obtain their consent to share their Sensitive Information with others.

C. The Meta Pixel

41. Meta's, f/k/a Facebook's, core business function is to sell advertising and it does so on several platforms, including Facebook and Instagram. The bulk of Meta's billions of dollars in annual revenue comes from advertising—a practice in which Meta actively participates through the use of algorithms that approve and deny ads based on the ads' content, human moderators that further review ads, for both legality and aesthetics prior to and after the ads are published, and other algorithms that connect ads to specific users, without the assistance or input of the advertiser.

42. Over the last decade, Meta has become one of the largest and fastest growing online advertisers in the world. Since its creation in 2004, Facebook's daily, monthly, and annual user base has grown exponentially to billions of users.

43. Meta's advertising business has been successful due, in significant part, to Meta's ability to target people its users, both based on information users provide to Meta, and other information about users Meta extracts from the internet at large. Given the highly specific data used to target specific users, thousands of companies and individuals utilize Facebook's advertising services.

44. One of Meta's most powerful advertising tools is the Meta Pixel, which Facebook first launched in 2015.

45. Meta branded Pixel as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website." Meta further stated:

> Facebook pixel, [is] a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website. We're also announcing the availability of custom conversions, a new rule-based method to track and report conversions for your Facebook ads.
>
> Facebook pixel makes things simple for advertisers by combining the functionality of the Conversion Tracking pixels and Custom Audience pixels into a single pixel. You only need to place a single pixel across your entire website to report and optimize for conversions. Since it is built on top of the upgraded Custom Audience pixel, all the features announced in our previous blog post (Announcing Upgrades to Conversion Tracking and Optimization at Facebook) are supported through Facebook pixel as well.
>
> [Advertisers and website operators] can use Facebook pixel to track and optimize for conversions by adding standard events (e.g., Purchase) to your Facebook pixel base code on appropriate pages (e.g., purchase confirmation page).[9]

46. Websites are hosted by computer servers, through which the entity in charge of the website exchanges communications with Internet users via their web browsers. The instructions that command the browser is called the source code. The source code can command a web browser to send data transmissions to third parties via pixels, which can allow a website to export data about users and their actions to third parties. The third parties receiving this data are typically configured to track user data and communications for marketing purposes.

[9] Cecile Ho, Announcing Facebook Pixel, Meta (Oct. 14, 2015) https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/.

47. The pixels are invisible to the website users and thus, without any knowledge, authorization or action by the user, the website site developer (website commander) can use it source code to contemporaneously and invisibility re-direct the user's PII and other non-public medical information to third parties.

48. Meta offers Pixel as a piece of code to integrate into websites, like Defendant's Website as among other things, a tool to help increase profits and revenue. As the name implies, Pixel "tracks the people and the type of actions they take."[10] According to Meta, Meta's Pixel is a piece of code that allows Defendant to "understand the effectiveness of [its] advertising and the actions [website visitors] take on [its] site."[11]

49. Through this technology, Meta intercepts each page a user visits, what buttons they click, as well as specific information they input into the website and what they searched. Pixel sends each of these pieces of information to Meta with PII, such as the user's IP address. Meta stores this data on its own servers, in some instances for years on end.

50. This data is often associated with the individual user's Facebook account. For example, if the user is logged into their Facebook account when the user visits Defendant's website, Meta receives third party cookies allowing Meta to link the data collected by Meta Pixel to the specific Facebook user.

51. Meta can also link the data to a specific user through the "Facebook Cookie." The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one

[10] Facebook, Retargeting, https://www.facebook.com/business/goals/retargeting.

[11] https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

developed by Apple, Inc., to track users, including Facebook users. Additionally, Meta can link User Data to individual users by identifying information collected through Meta Pixel through what Meta calls "Advanced Matching." There are two forms of Advanced Matching: manual matching and automatic matching. Using Manual Advanced Matching the website developer manually sends data to Meta to link users. Using Automatic Advanced Matching, the Meta Pixel scours the data it receives to search for recognizable fields, including name and email address to match users to their Facebook accounts.[12]

52. Pixel also allows Defendant to impact the delivery of ads, measure cross-device conversions, create custom audiences, learn about its website, and save money on advertising and marketing costs.[13] But, most relevant here, Pixel allowed Defendant and Meta to secretly track website users on Defendant's website and intercept their communications with Defendant. Indeed, Pixel is a bit of code that advertisers can integrate into their website, mobile applications and servers, thereby enabling Meta to intercept and collect user activity on those platforms.

53. As an example of this, consider again, an individual who navigates to Defendant's website and selects the tab for "Providers." When that tab is clicked, the individual's browser sends a GET request to Defendant's server requesting that server to load the webpage. Because Defendant employs Pixel on its website, Meta's embedded

[12] Meta uses the hashed format specifically to link Meta Pixel data to Facebook profiles. *See* Anson Chan, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022, 12:46 PM), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medicalinformation-from-hospital-websites.

[13] *Id.*

code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual it is happening.

54. Then, Meta causes the browser to secretly duplicate the website visitor's communication with Defendant, transmitting it to Meta's servers, alongside additional information that transcribes the communications' content and the individual's identity. Thus, when Plaintiff and the Class members visited Defendant's Websites and entered their Sensitive Information, or inquired about sensitive personal things, that information was transmitted to Meta, including but not limited to details like the physician and appointment selected, treatments and care options, and specific button/menu selections. During that same transmission, Defendant would also provide Meta with the patient's Facebook ID number, IP address or device ID or other personally identifying information. This information makes it easy to identify the patients through the collection of identifying information that was improperly disclosed.

55. Once Meta has the data, it can process it, analyze it, and assimilate it into databases like Core Audiences or Customer Audiences for advertising purposes. If the website visitor is also a Facebook user, Meta will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile. In sum, Pixel allows Meta to learn, and use for financial gain, the medical and private content Defendant's website visitors viewed on Defendant's website.

D. Defendant Employed Pixel on its Websites to Allow Meta to Intercept Communications and Class Members' Sensitive Information.

56. By employing Pixel on its website, Defendant shares its patients' and website visitors' identities and online activity, including private communications and search results related to private medical treatment.

57. A browsing session online may consist of thousands of website communications. Website communications include Requests (HTTP or HTTPS) and Responses (HTTP or HTTPS), and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.

a. An **HTTP Request** is an electronic communication a website visitor sends from his device's browser to the website's server. There are two types of HTTP Requests: (1) GET Requests, which are one of the most common types of HTTP Requests--in addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies; and (2) POST Requests which can send a large amount of data outside of the URL. In this case, a patient's HTTP Request would be asking Defendant's Website to get certain information, like a list of clinic locations or providers.

b. **Cookies** are a text file that website operators, and others use to store information on the visitor's device and these can later be communicated to a server or servers. Cookies are sent with HTTP Requests from website visitor's devices to the host server. Some cookies are "third party cookies"

which means they can store and communicate data when visiting one website to an entirely different website. Third party cookies are created by a website with a domain name other than the one the user is visiting, in this case Meta.[14] There are also "first party cookies," like the fbp cookie, which is created by the website the user is visiting, in this case Defendant.[15] Meta uses both first- and third-party cookies in Pixel to link FIDs and Facebook profiles. Defendant sent these identifiers to Meta.

c. An **HTTP Response** is a response to an HTTP Request. It is an electronic communication that is sent as a reply to the website visitor's device's web browser from the host server. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data. Basically, the HTTP Response is when the website sends the requested information (see the HTTP Request) and is sometimes called the "Markup."

58. A user's HTTP Request essentially asks the Defendant's Websites to retrieve certain information (such as a "Find Provider" page), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Websites).

[14] *Third-Party Cookie*, PCMAG.com, https://www.pcmag.com/encyclopedia/term/third-party-cookie. This is also confirmable using web developer tools to inspect a website's cookies and track network activity. This is confirmable by tracking network activity.

[15] *First-Party Cookie*, PCMAG.com, https://www.pcmag.com/encyclopedia/term/first-party-cookie. This is also confirmable using web developer tools to inspect a website's cookies and track network activity.

59. Websites, including Defendant's, also always include source code, which are the instructions and commands for the website and it requires the website visitor's browser to take certain actions when the web page loads and when the user makes certain requests of the webpage.

60. Source code can also command a web browser to transmit data to third parties in the form of an HTTP Request. This can be done quietly in the background without notifying the web browser's user. The Pixel Defendant uses is source code that does just that. The Pixel acts much like a traditional wiretap.

61. When users visit North Memorial's Websites via an HTTP Request to North Memorial's servers, that server sends an HTTP Response including the Markup that displays the Websites visible to the user and source code including the Pixel.

62. Thus, Defendant is, in essence, handing patients a tapped device and once the webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the webpage to trigger the tap, which intercepts those communications and transmits those communications to third parties, including Meta. Such conduct occurs on a continuous, and not sporadic, basis.

63. Third parties, like Meta, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user, in this case specifically identifying Plaintiff and the Class Members and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the personal information intercepted.

64. Thus, without any knowledge, authorization, or action by a user, Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly redirect the user's communications, including patient status, searches related to private medical treatment, and other online activity, to third parties. divulges

65. Using the same example as before, when a user visits Defendant's website, www.northmemorial.com, to search for a doctor needed for a particular private treatment or condition, they may select the "Find a Doctor" tab, which takes them to the "Find a Doctor Page."

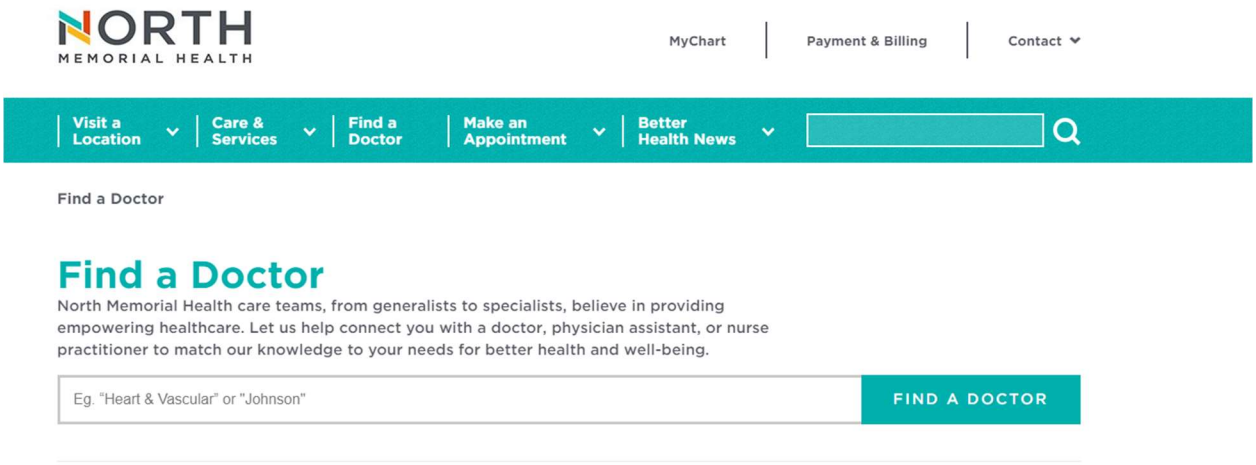


Figure 1. Defendant directs patients to its "Find a Doctor" webpage with embedded Pixel.

66. If the patient or website visitor researching a particular private treatment or condition selects filters or enters keywords into the search bar on the "Find a Doctor" webpage, the filters and search terms are transmitted via Meta's Pixel. Additionally, if a patient or website visitor uses the Website's general search bar or chat, the terms and phrases the patient or visitor types are transmitted to Meta, even if they contain a website

visitor's private treatment, procedure, medical conditions, and related inquiries. This information is automatically sent from the website visitor's device to Meta, and it reveals the individual's FID along with each search filter the patient selected.

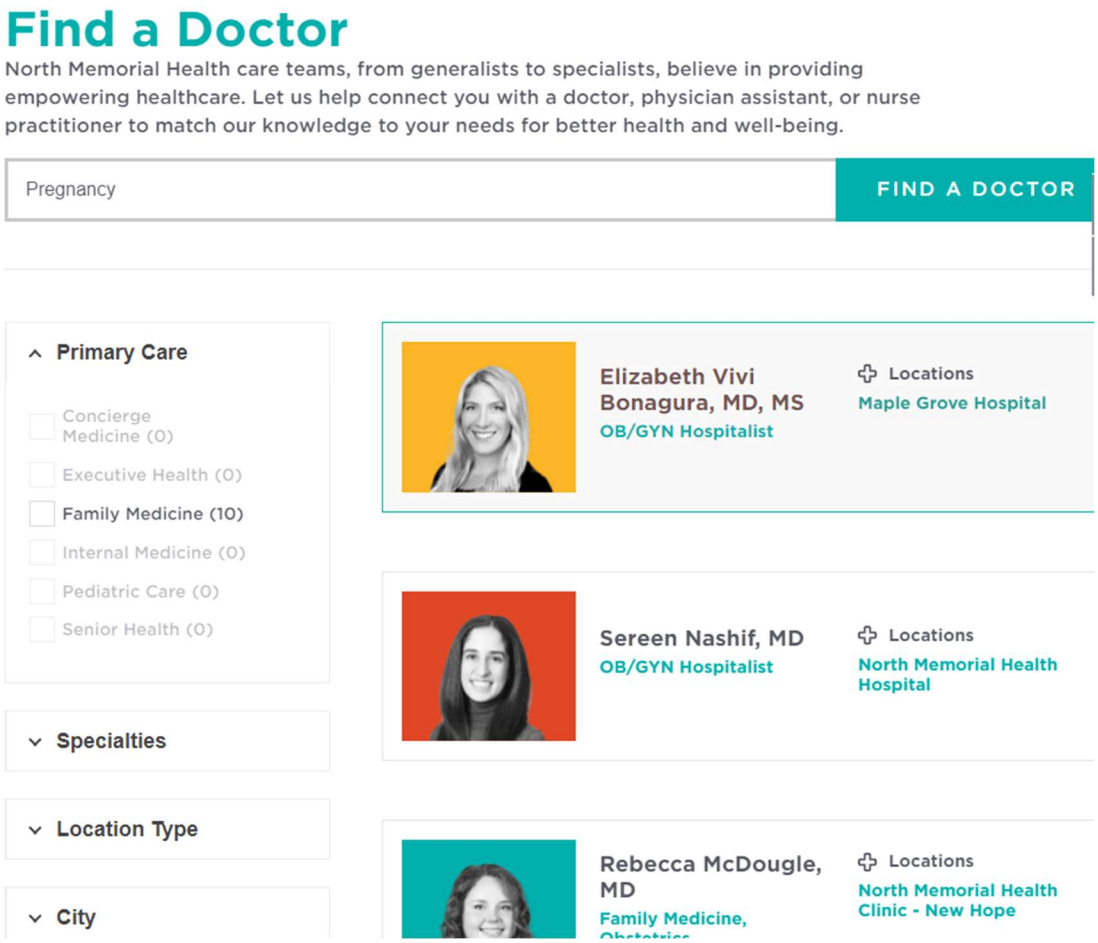


Figure 2. Example of search results for a provider specializing in "Pregnancy."

67. As an example, after submitting "Pregnancy" in the search bar on the "Find a Doctor" webpage, website visitors are directed to the search results page, and their selections or search parameters are automatically transmitted to Meta.

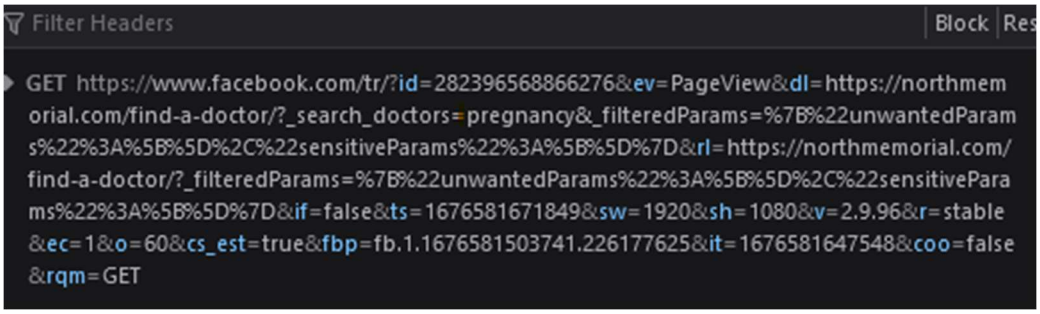


Figure 3. Example of data from a search result for "Pregnancy" provider being shared with Facebook.

68. Defendant's website also includes a feature that allows patients to book appointments related to a particular private treatment or condition. If a patient or potential patient clicks on the "Make an Appointment" button, this action is communicated and shared with Meta. Each selection the patient or potential patient selects in relation to making their appointment is communicated to Meta.

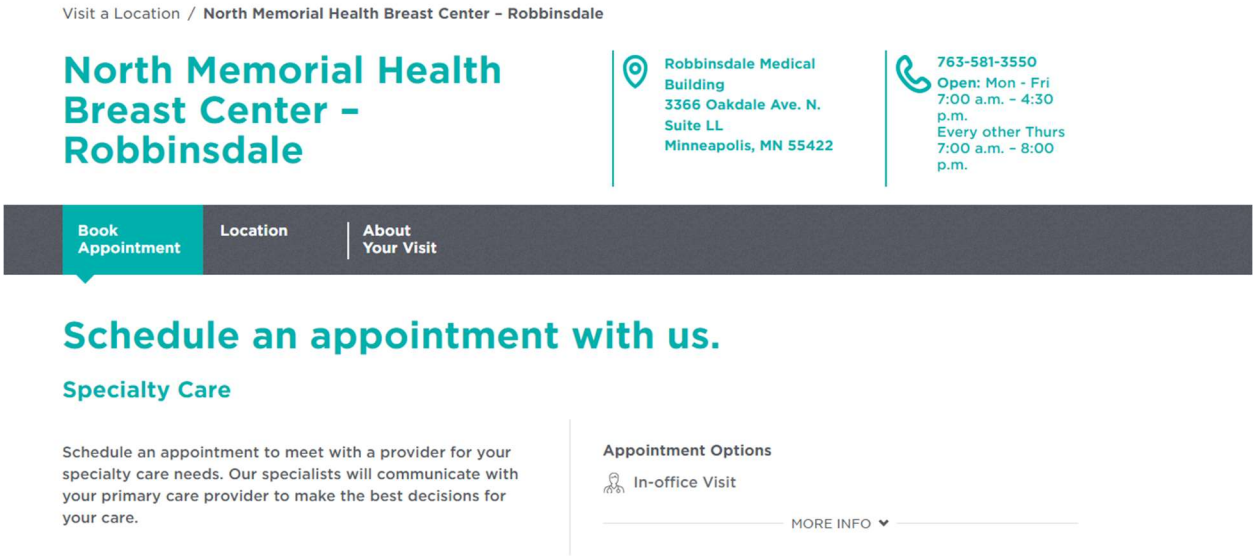


Figure 4. Example of Defendant's webpage after a website visitor selects the North Memorial Health Breast Center, Robbinsdale for the location of her appointment.

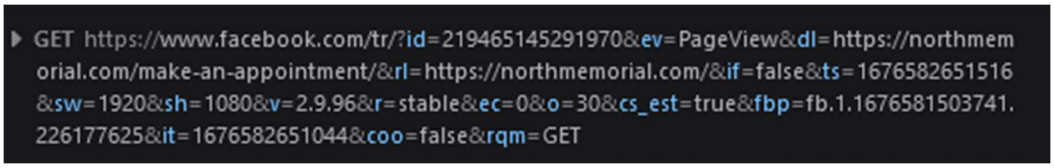
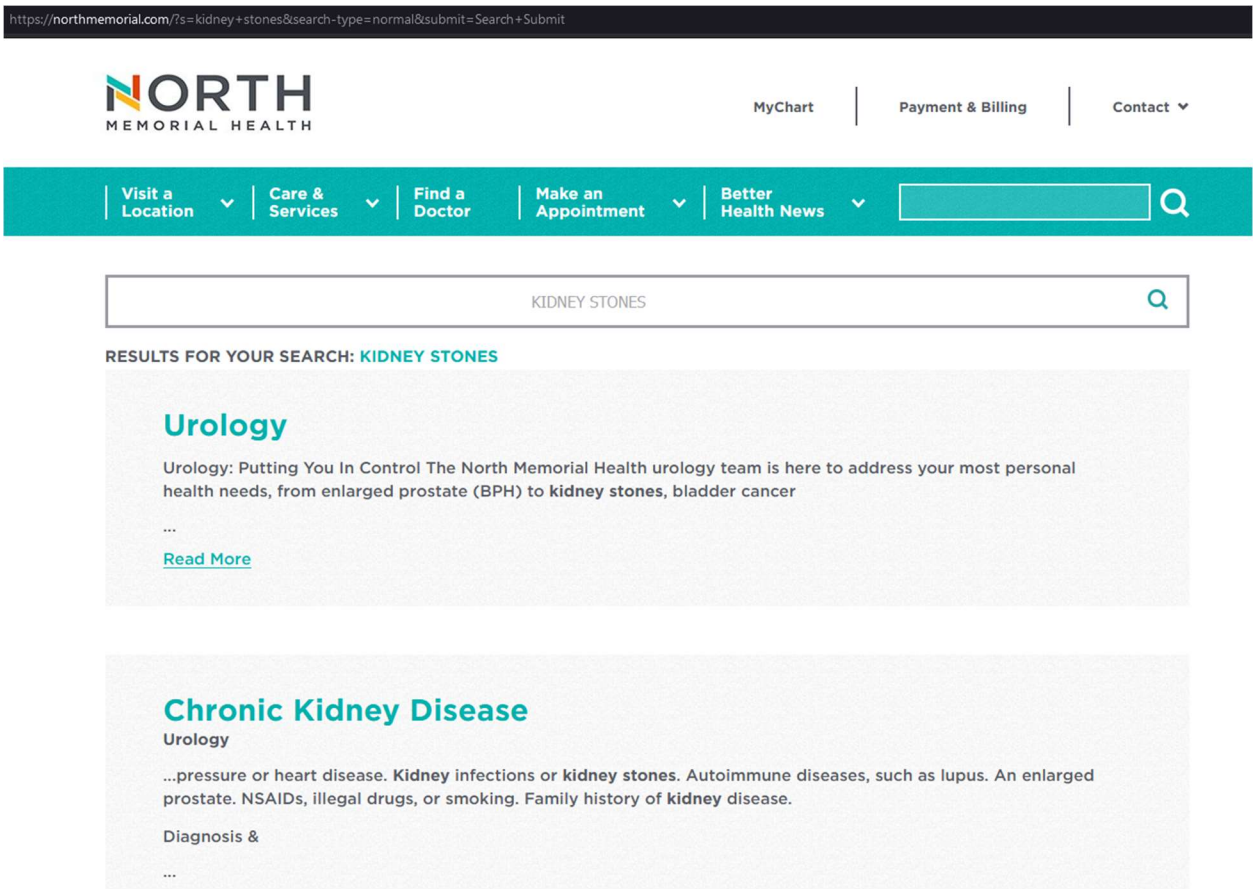
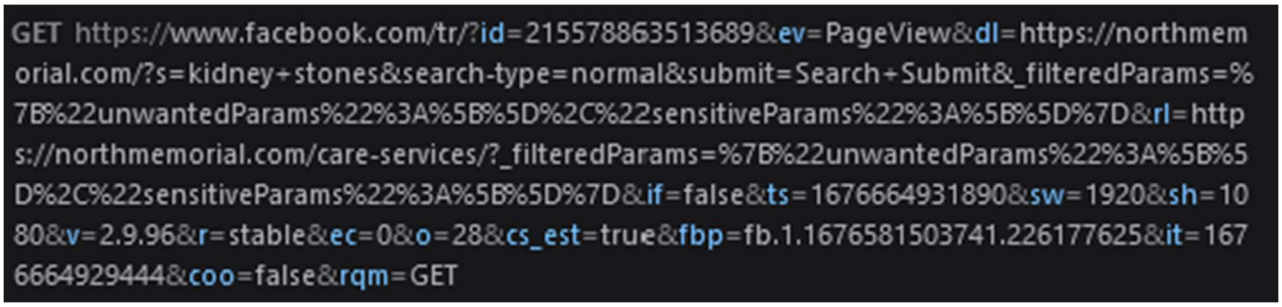


Figure 5. Example of data from Robbinsdale location selection being transmitted to Meta.

69. Looking at Figure 5, Defendant's source code secretly instructs the website visitor's browser to duplicate the visitor's communications and send those communications to Meta with an identifier, so that the information can be linked to an actual person. This occurs in real-time.

70. Below is an example of a search for kidney stones and the transmission of that search communication to Meta, with an identifier.





71. The above screenshots demonstrate the real-time transmission of personal information, and in this example, related to symptoms of a condition, that is being shipped to Meta at Defendant's request.

72. Installing Pixel effectively opens a spying window through which the webpage can funnel visitor data, actions and communications to third parties. Defendant's source code manipulates website visitor's browsers by secretly instructing it to duplicate the Website Communications and sending those communications to Meta. Thus, without website users' consent, Defendant has effectively used its source code to commandeer website users' computing devices thereby redirecting private communications.

73. Each time Defendant transmits this data to Meta, it also discloses the patient's personally identifiable information. Additionally, each time a user who accesses Defendant's website while logged (or recently having logged) in Facebook will transmit a cookie, or multiple cookies to Facebook, which contains that user's unencrypted Facebook ID. Defendant utilized the fbp cookie, among others, which attaches to a browser as a first-party cookie and which Meta uses to identify a browser and a user.[16]

[16] Facebook.com, Cookies & Other Storage Technologies, https://www.facebook.com/policy/cookies/

74. Plaintiff and the Class members never consented, authorized, or otherwise permitted Defendant to disclose their personally identifiable and protected health information to third parties, including Meta. Plaintiff was not provided with any prior written notice that Defendant disclosed her Website Communications, nor was she provided any means of opting out of such disclosures. Even so, Defendant knowingly and intentionally disclosed Plaintiff's and the Class Members' protected and private information.

E. Exposure of Sensitive Information Creates a Substantial Risk of Harm

75. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[17]

76. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require, among other things: (1) using industry tested and accepted methods; (2) monitoring activity on networks

[17] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022) https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

to uncover unapproved activity; (3) verifying that privacy and security features function properly; and (4) testing for common vulnerabilities or unauthorized disclosures.[18]

77. The FTC cautions businesses that failure to protect Sensitive Information and the resulting privacy breaches can destroy consumers' finances, credit history, and reputations, and can take time, money and patience to resolve the effect.[19] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

F. Plaintiff's and the Class's Sensitive Information is Valuable.

78. As many healthcare data industry experts have recognized, "[p]atients' medical data constitutes a cornerstone of the big data economy. A multi-billion-dollar industry operates by collecting, merging, analyzing and packaging patient data and selling it to the highest bidder."[20]

79. The personal, health, and financial information of Plaintiff and the Class is valuable and has become a highly desirable commodity. Indeed, one of the world's most valuable resources is the exchange of personal data.[21]

---

[18] *Start With Security, A Guide for Business,* FTC (last visited Jan. 18, 2022) https://www.ftc.gov/business-guidance/resources/start-security-guide-business

[19] *See* Taking Charge, What to Do if Your Identity is Stolen, FTC, at 3 (2012) (last visited Jan. 19, 2022), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf

[20] Yaraghi, Niam, *Who should profit from the sale of patient data?,* The Brookings Institution, Nov. 19, 2018, https://www.brookings.edu/blog/techtank/2018/11/19/who-should-profit-from-the-sale-of-patient-data/ (last visited March 18, 2023).

[21] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

80. Business News Daily reported that businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, consumer interaction with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, consumer satisfaction data) from consumers.[22] Companies then use this data to impact the customer experiences, modify their marketing strategies, publicly disclose or sell data, and even to obtain more sensitive data that may be even more lucrative.[23]

81. The power to capture and use customer data to manipulate products, solutions, and the buying experience is invaluable to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[24]

82. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[25] In this paper, the OECD

[22] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUSINESS NEWS DAILY (Aug. 5, 2022; updated Aug. 25, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[23] *Id.*

[24] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, MCKINSEY (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[25] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220, OECD PUBLISHING PARIS, (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

measured prices demanded by companies concerning user data derived from "various online data warehouses."[26]

83. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[27]

84. Unlike financial information, such as credit card and bank account numbers, the PHI and certain PII cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable.[28]

85. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal

[26] *Id.* at 25.

[27] *Id.*

[28] *Calculating the Value of a Privacy Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Jan. 18, 2022).

information is worth between $30.49 and $44.62.[29] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

86. Defendant's privacy violations exposed a variety of Sensitive Information, including medical histories, prescription information, communications with medical professionals, dates of birth, medical insurance information, and other highly sensitive data.

87. It is important to note that the Social Security Administration ("SSA") warns that the unauthorized disclosure of a Social Security number can lead to identity theft and fraud.[30]

88. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

89. PHI, like that exposed here, is likely even more valuable than Social Security numbers and just as capable of being misused.[31] PHI can be ten times more valuable than

[29] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore,* at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 19, 2022).

[30] Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited Jan. 19, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[31] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-healthcare-cyber-intrusions/ (last visited Jan. 18, 2022).

credit card information.[32] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, social security numbers.[33]

90. Indeed, prescription records, blood tests, doctor notes, hospital visits and insurance records are all sold to commercial companies, which gather years of health information on hundreds of millions of people and then sell it to other industries, like pharmaceutical companies who use the information to sell more drugs.[34] Some industry insiders and journalists are even calling hospitals the "brokers to technology companies" for their role in data sharing in the $3 trillion healthcare sector.[35] "Rapid digitization of health records … have positioned hospitals as a primary arbiter of how much sensitive data is shared."[36]

[32] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[33] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 18, 2022).

[34] Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Industry*, TIME, (Jan. 9, 2017), https://time.com/4588104/medical-data-industry/.

[35] Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records*, The Wall Street Journal, (Jan. 20, 2020), https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200.

[36] *Id.*

G. Plaintiff and the Class Had a Reasonable Expectation of Privacy in Their Interaction with Defendant's Website and Application.

91. Consumers are concerned about companies, like Defendant, collecting their data and assume the data they provide, particularly highly sensitive medical and insurance data, will be kept secure and private.

92. In a recent survey related to internet user expectations, most website visitors stated they assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[37] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[38]

93. The majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its' customers' data.[39] In fact, the overwhelming majority of Americans equate personal privacy as important as concerns about crime, access to quality healthcare, and the future of the social security system.[40]

94. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and Website should be required to obtain consent before selling or

---

[37] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.

[38] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, THE INFORMATION SOCIETY, 38:4, 257, 258 (2022).

[39] *Public Opinion on Privacy*, EPIC.ORG, https://archive.epic.org/privacy/survey/.

[40] *Freedom of Information in the Digital Age*, AMERICAN SOCIETY OF NEWSPAPER EDITORS FREEDOM OF INFORMATION COMMITTEE AND THE FIRST AMENDMENT CENTER, (April 3, 2001).

sharing consumers' data, and the same percentage believe internet companies and Website should be required to provide consumers with a complete list of the data that has been collected about them.[41]

95. A March 2000 BusinessWeek/Harris Poll found that 89% of respondents were uncomfortable with web tracking schemes where data was combined with an individual's identity.[42] The same poll found that 63% of respondents were uncomfortable with web tracking even where the clickstream data was not linked to personally identifiable information.[43] A July 2000 USA Weekend Poll showed that 65% of respondents thought that tracking computer use was an invasion of privacy.[44]

96. Patients and website users act consistently with their expectation of privacy. For example, following a new rollout of iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[45]

---

[41] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumer-reports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/.

[42] *Public Opinion on Privacy*, EPIC.ORG, https://archive.epic.org/privacy/survey/.

[43] *Id.*

[44] *Id.*

[45] Margaret Taylor, *How Apple screwed Facebook*, WIRED, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

97. Like the greater population, certainly, Defendant's patients would expect the highly sensitive *medical* information they provided to Defendant, through the website or other applications, to be kept secure and private.

H. Defendant's Conduct Violated HIPAA

98. Under HIPAA, individuals' health information must be:

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.[46]

99. HIPAA is a "federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[47] The rule requires appropriate administrative, physical, and technological safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[48]

100. HIPAA defines "protected health information" as "individually identifiable" information that is "created or received by a health care provider" (or similar entities) that

[46] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Aug. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[47] *Health Insurance Portability and Accountability Act of 1996 (HIPAA),* Centers for Disease Control and Prevention (last visited Aug. 19, 2022) https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20(HIPAA),-On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

[48] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Aug. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

"[r]elates to past, present, or future physical or mental health or conduction of an individual" or the "provision of health care to an individual." 45 C.F.R. § 160.103. Identifiers such as patient-status (*i.e.*, information that connects a particular user to a particular healthcare provider), gathered in this case by Pixel through the sign in button on North Memorial's website homepage or the actual login to North Memorial's patient portal, constitute protected health information.

101. Additionally, HIPAA defines sensitive patient personal and health information as: (1) Name; (2) Home and work addresses; (3) Home and work phone numbers; (4) Personal and professional email addresses; (5) Medical records; (6) Prescriptions; (7) Health insurance information; (8) Billing information; (9) Social Security number; (10) Spouse and children's information; and/or (11) Emergency contact information.[49]

102. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data Defendant failed to protect. The Privacy violations described herein resulted from Defendant's failure to comply with several of these standards:

a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits;

b. Violation of 45 C.F.R. § 164.312(a)(1): Failing to implement technological policies and procedures for electronic information

[49] *What is Considered Protected Health Information Under HIPAA*, HIPAA Journal, Jan. 2, 2022: U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Aug. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Aug. 19, 2022).

systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;

c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

d. Violation of 45 C.F.R. §164.306(a)(2): Failing to protect against any reasonably–anticipated threats or hazards to the security or integrity of electronic protected health information;

e. Violation of 45 C.F.R. §164.306(a)(3): Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

f. Violation of 45 C.F.R. §164.306(a)(94): Failing to ensure compliance with HIPAA security standard rules by its workforce;

g. Violation of 45 C.F.R. §164.502, *et seq*: Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons; and

h. Violation of 45 C.F.R. §164.530(c): Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information.

103. Additionally, according to Health and Human Services' Health Information Privacy Bulletin ("HHS Privacy Bulletin"), HIPPA covered entities cannot share PII or PHI to online tracking technology vendors for marketing purposes without first obtaining the individual's HIPAA compliant authorization.[50] The HHS Privacy Bulletin explicitly states:

[50] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES, (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

> The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.

HHS Privacy Bulletin (internal citations omitted)(emphasis in original)[51].

104. The HHS Privacy Bulletin also identifies several harms that may result from an impermissible disclosure of an individual's PHI, including:

> identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.

HHS Privacy Bulletin (internal citations omitted)(emphasis in original)[52].

105. According to HHS, HIPAA "[r]egulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website, including individually identifiable health information that the individual provides when they use regulated entities' websites." The information an

[51] *Id.*

[52] *Id.*

individual provides may include a medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code.[53]

106. All of the above listed information that is collected on a regulated entity's website, like Defendant's websites, is PHI, "even if the individual does not have an existing relationship with the regulated entity and even if the [information], such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services." When a regulated entity, again like Defendant, collects the individual's information, that information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[54]

I. Defendant's Privacy Policy Does Not Excuse its Use of Pixel.

107. Defendant has a Notice of Privacy Practices[55] and a Website Privacy Policy ("Privacy Policy")[56]. A link to the Privacy Policy can be found on the North Memorial website homepage, northmemorial.com, at the bottom of the page. There is no pop-up link, or other notification advising website users to visit the Privacy Policy before interacting

[53] *Id.*

[54] *Id.*

[55] https://northmemorial.com/wp-content/uploads/2017/03/North-Memorial-Health-notice_of_privacy_practices_2017.pdf.

[56] https://northmemorial.com/privacy-policy/.

with the website. The existence of these policies does not authorize North Memorial to share Plaintiff's and the Class Members' Sensitive Information with Meta.

108. The Privacy Policy includes the following representations[57]:

a. We protect health and medical information as required by federal and state privacy laws.
b. North Memorial is committed to ensuring that your privacy is protected.
c. We may disclose information to third parties who act for us or on our behalf.
d. We are committed to ensuring that your information is secure. In order to prevent unauthorized access or disclosure we have put in place appropriate physical, electronic and managerial procedures to safeguard and secure the information we collect online.

109. North Memorial also admits to the use of cookies on its website. Specifically, Defendant uses "cookies to identify which pages are being used."[58] North Memorial further represents that "[a] cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us."[59]

110. Cookies are distinct from pixels and are in fact two completely different kinds of technology. Cookies are small text files containing a limited amount of information which sit idly on a user's computer until contacted by a server. Pixel, on the other hand, captures an individual's data in a manner that is much more active and invasive than cookies.

111. There are two kinds of cookies, first- and third-party cookies. The primary difference between first- and third- party cookies is who owns the cookies. First-party

[57] *Id.*
[58] *Id.*
[59] *Id.*

cookies are owned by the website, while third-party cookies belong to a website other than the one a user is currently viewing.

112. First-party cookies like those on North Memorial's Websites, are designed to collect information that can help the website owner improve their site. These cookies are used for things like saving user settings or saving a shopping cart. For example, first party cookies cannot follow users across devices, the information is placed on the user's browser, and these cookies can be blocked or cleared by users from the browser settings. In North Memorial's Privacy Policy, it identifies the use of cookies to identify which pages are being used on the Websites. Specifically, it states it uses cookies to "identify which pages are being used." This is evident of the use of a first-party cookie.

113. Third-party cookies are set up by a third-party server, such as Meta. These cookies are used to identify a specific person who is using a particular website and carry this information between websites so that you see how the user is moving through the internet. North Memorial makes no disclosures in its Privacy Policy related to third-party-cookies.

114. Pixel does more than either first- or third-party cookies because it collects, in real-time, information about the user's browser and system configuration. Additionally, tracking pixels, like Pixel, can follow users across devices, the user's information and Website Communications are sent directly to third party web servers from the user's device, users do not know the Pixel is installed and it is not easily disabled by the end-user.

115. The Privacy Policy does not mention Pixel or describe its unfettered interception of all of Plaintiff's and the Class Members' Website Communications and

real-time transmission of those communications to Meta. Meta is an independent entity from North Memorial and uses the data it collects via the Pixel for its own purposes, unrelated to North Memorial. No reasonable person could ascertain from the Privacy Policy that their private, HIPAA-protected health data was being collected and shipped to Meta for purposes unrelated to their medical care.

116. Moreover, the Privacy Policy is not readily available to users when they open the North Memorial website, northmemorial.com, and the mere existence of the Privacy Policy on the Websites cannot confer consent to its terms. Additionally, the actual terms of the Privacy Policy do not confer authorization by the users to disclose Sensitive Information, including medical information, to third party Meta via Pixel. Indeed, the terms of the Privacy Policy state "[b]y using this website, you are consenting to the collection, use, and disclosure of your information as described in this policy". The information described in the policy includes name, contact information including email address, demographic information such as zip code, preferences and interests, and other information relevant to participation in a course, tour or even in the case of online class, even registration or consumer sweepstakes.[60] This disclosure certainly does not provide North Memorial unlimited authorization to send Meta all of Plaintiff's and the Class Members' Website Communications, including HIPAA-protected information, like it does.

117. From the Privacy Policy, users can access a link to the Notice of Privacy Practices ("Notice"). The Notice identifies the following purposes for disclosing patients'

[60] https://northmemorial.com/privacy-policy/.

medical information: treatment, health care operations, hospital directories, and to inform family members or friends who will be caring for the patient or paying the patient's medical bills. [61] Other disclosures are only to be made with written authorization. [62] This Notice certainly does not provide North Memorial unlimited authorization to send Meta all of Plaintiff's and the Class Member'' Website Communications, like it does.

118. In fact, according to 45 CFR 104.508(c)(1), for a HIPAA authorization to be valid, it must:

a. Describe the specific PHI the patient is authorizing to be shared;

b. Name the entities authorized to make the disclosure;

c. Name the persons or entities to whom disclosure may be made;

d. Contain an expiration date; and

e. Contain a signature and date.

Defendant's Privacy Policy or Notice do not satisfy any of these requirements and cannot be considered a waiver of HIPAA rights or an authorization by Plaintiff and the Class allowing Defendant to share their personal information with Meta.

CLASS ALLEGATIONS

119. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23 on behalf of themselves and all others similar situated, as representative of the following Class:

Nationwide Class:

[61] https://northmemorial.com/wp-content/uploads/2017/03/North-Memorial-Health-notice_of_privacy_practices_2017.pdf.

[62] *Id.*

All persons whose Sensitive Information was disclosed to a third party through Defendant's Website without authorization or consent.

120. Excluded from the Class are Defendant; its officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest in, is a parent or subsidiary of, or which is otherwise controlled by Defendant; and Defendant's affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assignees. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

121. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

122. All members of the proposed Class are readily identifiable through Defendant's records.

123. **Numerosity.** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes at least 1.5 million people. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

124. **Commonality and Predominance.** This action involves common questions of law and fact to the Plaintiff and Class members, which predominate over any questions only affecting individual Class members. These common legal and factual questions include, without limitation:

a. Whether Defendant owed Plaintiff and the other Class members a duty to adequately protect their Sensitive Information;

b. Whether Defendant owed Plaintiff and the other Class members a duty to secure their Sensitive Data from third-party tracking technologies provided by Meta;

c. Whether Defendant owed Plaintiff[s] and the other Class members a duty to implement reasonable data privacy protection measures because Defendant accepted, stored, created, and maintained highly sensitive information concerning Plaintiff and the Class;

d. Whether Defendant knew or should have known of the risk of disclosure of data through third party tracking technologies;

e. Whether Defendant breached its duty to protect the Sensitive Information of Plaintiff and other Class members;

f. Whether Defendant knew or should have known about the inadequacies of its privacy protection;

g. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized disclosure;

h. Whether proper data security measures, policies, procedures and protocols were enacted within Defendant's offices and computer systems to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized disclosure;

i. Whether Defendant's conduct was the proximate cause of Plaintiff's and the Class's injuries;

j. Whether Plaintiff and the Class suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;

k. Whether Plaintiff and the Class are entitled to recover damages; and

l. Whether Plaintiff and the Class are entitled to other appropriate remedies including injunctive relief.

125. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of herself and the Class. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

126. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's Sensitive Information, like that of every other Class member, was improperly disclosed by Defendant. Defendant's misconduct impacted all Class members in a similar manner.

127. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interest of the members of the Class and has retained counsel experienced in complex consumer class action litigation and intend to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

128. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. The adjudication of this controversy through a class action will avoid the

possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court.

CLAIMS

COUNT I
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA") (18 U.S.C. § 2511(1))
(On behalf of Plaintiff and the Nationwide Class)

129. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

130. The ECPA protects against the intentional interception, attempted interception, or the procurement of another person to intercept or attempt to intercept any wire, oral, or electronic communication. *See* 18 U.S.C. § 2511(1)(a).

131. The ECPA further provides any person who

> (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—
>
> (i)such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication;
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

> Shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2511(1) (b), (c) & (d).

132. Pursuant to 18 U.S.C. § 2511(5)(b), for violations of the ECPA, the Court "may use any means within its authority to enforce an injunction issued under paragraph (ii)(A) and shall impose a civil fine of not less than $500 for each violation of the injunction. Additionally, 18 U.S.C. § 2520 provides that "any person whose wire, oral or electronic communication is intercepted, disclosed or intentionally used in violation of Chapter 119, may recover from the person or entity that engaged in the violation in a civil action.

133. The ECPA protects against both the sending and receipt of communications.

134. The transmission of Plaintiff's and the Class members' Sensitive Information violates the ECPA. First, the transmissions from Plaintiff and the Class members to Defendant, through Defendant's Website (www.northmemorial.com) are communications pursuant to 18 U.S.C. § 2510(12).

135. "Interception" means "the acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents… include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C.§ 2510(4), (8).

136. "Content", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication 18 U.S.C.§ 2510(8).

137. "Intercepting device" or the "Electronic, mechanical or other device" means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication. U.S.C.§ 2510(5). Here, Plaintiff's and the Class members' browsers and computing devices and Defendant's webservers, website, and the Pixel code Defendant deployed are all "devices" for the purposes of the ECPA.

138. "Electronic communication" means *any communication* made in whole or in part through the use of facilities for the transmission of communications by the signs, signals, writing or data between the point of origin and the point of reception. U.S.C.§ 2510(2).

139. By employing and embedding the Pixel on Defendant's Websites, Defendant intentionally violated the ECPA, through its interception, attempt at interception, and its procurement of Meta to intercept the electronic communications of Plaintiff and the Class members. Indeed, Defendant willfully used or attempted to use the contents of Plaintiff's and the Class Members' electronic communications, knowing that the information was obtained through interception. Defendant's use of confidential and private patient information and data for advertising and other revenue generating benefits, in the absence of express written consent, is intentionally criminal and tortious where the conduct violates state law, including invasion of privacy and intrusion upon seclusion.

140. Defendant's use of the Pixel unlawfully and intentionally disclosed Plaintiff's and the Class members' Sensitive Information to Meta, including but certainly not limited to, information regarding treatments, medications, scheduling, location,

procedures, test results, and diagnosis. These intentional acts violate 18 U.S.C. §§ 2511(1)(a), 2511(1)(c), 2511(1)(d).

141. Additionally, Defendant had no legitimate purpose for intentionally intercepting the contents of Plaintiff's and the Class members' private, and personal electronic communications. And even if Defendant could identify *some* legitimate purpose, which seems highly unlikely, it would not outweigh the egregious breach and invasion of privacy Defendant has committed against Plaintiff and the Class members.

142. At no time did Plaintiff and the Class members provide their consent to Defendant's disclosure of their Sensitive Information to Meta and/or other third-parties.

143. Further, Defendant has improperly profited from its invasion of Plaintiff's and the Class members' privacy in its use of their data for its economic value.

144. By embedding the Pixel on its Websites and disclosing the content of patient communications relating to medical research, patient portals, appointments and other sensitive information, North Memorial had a purpose that was tortious, criminal, and designed to violate state laws including:

a. A knowing intrusion into a private place or matter that would be highly offensive to a reasonable person;

b. A violation of 42 U.S.C. § 1320-6, the Administrative Simplification subtitle of HIPAA, which protects against the disclosure of individually identifiable health information to another person and is a criminal offense punishable by fine or imprisonment; and

c. Violation of HIPAA.

145. North Memorial knew that such conduct would be highly offensive and proceeded to embed Pixel and use it to the detriment of visitors to the Websites anyways.

146. Plaintiff and the Class members are entitled to damages, including compensatory and/or nominal damages in an amount to be proven at trial.

147. To the extent Defendant's conduct is ongoing, and it continues to unlawfully disclose the communications of Plaintiff and the Class members any time they use or provide information to Defendant through its Websites or application without their consent, Plaintiff and the Class members are entitled to declaratory and injunctive relief. This will prevent future unlawful and unauthorized disclosure of Plaintiff's and the Class members' Sensitive Information.

COUNT II
VIOLATION OF THE MINNESOTA WIRETAP STATUTE
Chapter 626A.02
(On behalf of Plaintiff and the Nationwide Class)

148. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

149. The Minnesota Wiretap Statute, Minn. Stat. 626A, protects against the intentional interception, attempted interception, or the procurement of another person to intercept or attempt to intercept any wire, oral, or electronic communication. *See* Minn. Stat. 626A.02, Subd. 1.

150. The Minnesota Wiretap Statute further provides any person who:

> (2) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

> (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
> (ii) such device transmits communications by radio, or interferes with the transmission of such communication;
>
> (3) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (4) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> Shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

Minn. Stat. 626A.02.

151. Additionally, a person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of Chapter 626A may recover from the person or entity that engaged in violation:

> 1. Temporary and other equitable or declaratory relief as may be appropriate;
> 2. Damages under subd. 3 …; and
> 3. A reasonable attorney's fee and other litigation costs reasonable incurred.

Minn. Stat. 626A.13, Subd. 2

152. The transmission of Plaintiff's and the Class members' Sensitive Information violates the Minnesota Wiretap Act. First, the transmissions from Plaintiff and the Class members to Defendant, through Defendant's Website (www.northmemorial.com and www.northmemorial.com/mychart-medical-records/) are wire communications pursuant to

Minn. Stat. 626A.01, Subd. 3.

153. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Minn. Stat. 626A.01, Subd. 5.

154. "Contents" means "when used with respect to any wire, electronic, or oral communication, includes any information concerning the substance, purport, or meaning of that communication." Minn. Stat. 626A.01, Subd. 8.

155. "Electronic, mechanical or other device" means any device or apparatus which can be used to intercept a wire, electronic, or oral communication. Minn. Stat. 626A.01, Subd. 6. Here, Plaintiff's and the Class members' browsers and computing devices and Defendant's webservers, website, and the Pixel code Defendant deployed are all "devices" for the purposes of the Minnesota Wiretap Statute.

156. "Electronic communication" means transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system but does not include:

(1) a wire or oral communication;

(2) a communication made through a tone-only paging device; or

(3) a communication from a tracking device, defined as an electronic or mechanical device which permits the tracking of the movement of a person or object.

Minn. Stat. 626A.01, Subd. 14.

157. By employing and embedding Pixel on Defendant's website, Defendant

intentionally violated the Minnesota Wiretap Statute, through its interception, attempt at interception, and its procurement by Meta to intercept the electronic communications of Plaintiff and the Class members.

158. Indeed, Defendant willfully used or attempted to use the contents of Plaintiff's and the Class members' electronic communications, knowing that the information was obtained through interception.

159. Defendant's use of Pixel unlawfully and intentionally disclosed Plaintiff's and the Class members' Sensitive Information to Meta, including but certainly not limited to, information regarding treatments, medications, scheduling, location, procedures, test results, and diagnosis. These intentional acts violate Minn. Stat. 626A.02.

160. Additionally, Defendant had no legitimate purpose for intentionally intercepting the contents of Plaintiff's and the Class members' private, and personal electronic communications. And even if Defendant could identify *some* legitimate purpose, which seems highly unlikely, it would not outweigh the egregious breach and invasion of privacy Defendant has committed against Plaintiff and the Class members.

161. At no time did Plaintiff and the Class members provide their consent to Defendant's disclosure of their Sensitive Information to Meta and/or other third-parties.

162. Further, Defendant has improperly profited from its invasion of Plaintiff's and the Class members' privacy in its use of their data for its economic value.

163. Plaintiff and the Class members are entitled to damages, including compensatory and/or nominal damages in an amount to be proven at trial.

164. To the extent Defendant's conduct is ongoing, and it continues to unlawfully

disclose the communications of Plaintiff and the Class members any time they use or provide information to Defendant through its Websites or application without their consent, Plaintiff and the Class members are entitled to declaratory and injunctive relief. This will prevent future unlawful and unauthorized disclosure of Plaintiff's and the Class members' Sensitive Information.

165. Pursuant to Minn. Stat. 626A.13, Subd. 3, the Court may assess damages by: (1) the sum of three times the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, whichever is greater of option (1) and option (2).

166. As a direct and proximate result of Defendant's conduct and pursuant to the Minnesota Wiretap Act, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; and reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT III
VIOLATION OF THE MINNESOTA CONSUMER FRAUD ACT
Minn. Stat. § 325F.69 *et seq*
(On behalf of Plaintiff and the Nationwide Class)

167. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

168. Defendant's practices were and are in violation of Minnesota's Consumer Fraud Act, Minnesota Statutes § 325F.69, *et seq.*

169. Defendant is a person as defined by Minnesota Statute § 325F.68, subd. 3.

170. The medical services that Defendant markets, provides, offers, and/or sells are considered merchandise. Minnesota Statute §325F.69, Subd. 2.

171. As alleged, Defendant engaged in deceptive acts and practices in the form of misrepresentations and omissions while conducting business throughout Minnesota to thousands of individuals seeking medical care. Specifically, Defendant represented that it lawfully, and in accordance with healthcare standard practices, protected the confidentiality and privacy of its patients and also omitted material information regarding its use of Meta Pixel on its website to the public at large. Defendant did not protect the confidentiality or privacy of its patients and it does in fact use Meta Pixel on its website which the general public can access online.

172. Defendant did not disclose its use of the Meta Pixel on its website or that it was sharing private, sensitive patient data with third-party Meta without the patients' consent. Defendant's failure to inform patients or potential patients of its use of Meta Pixel on its website and its disclosure of patient and website visitors' data to third parties was likely to, and did, deceive Plaintiff and the Class members.

173. As a direct result of Defendant's unlawful deceptive practices, Plaintiff and the Class members suffered injuries including the loss of their personal, private data.

174. Plaintiff and the Class members seek an award of damages for violations of Minn. Stat. § 325.69 pursuant to Minn. Stat. § 8.31, subd. 3a and all other appropriate relief.

COUNT IV
VIOLATION OF MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT ("MUDTPA") § 325D.43-48
(On behalf of Plaintiff and the Nationwide Class)

175. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

176. Defendant is subject to the rules and statutory requirements of Minn. Stat. § 325D.44, because it advertised, offered, or sold goods or services in Minnesota and therefore engaged in business directly or indirectly affected people in Minnesota.

177. The MUDTPA prohibits deceptive trade practices in a person's business, vocation, or occupation, *See* Minn. Stat. § 325D.44, subd. 1, including where the person:

> represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that the person does not have; Minn. Stat. § 325D.44, subd.1(5).

> represents that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; Minn. Stat. § 325D.44, subd.1(7).

178. Defendant engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Sections Minn. Stat. § 325D.44, subd. 1(5) & (7).

179. Defendant's misrepresentations and omissions include both implicit and explicit representations through:

a. Failing to implement and maintain reasonable privacy measures to protect Plaintiff's and the Class's Sensitive Information, which was a direct and proximate cause of the Privacy violations described herein;

b. Failing to identify and remediate foreseeable privacy risks and adequately maintain privacy measures despite knowing the risk disclosure of patients' Sensitive Information, which was a direct and proximate cause of the Privacy violations;

c. Failing to comply with common law and statutory duties pertaining to the privacy of Plaintiff's and the Class's Sensitive Information, including duties imposed by the HIPAA, 45 C.F.R. § 160.102 and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Privacy violations;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class's Sensitive Information, including by implementing and maintaining reasonable privacy protection measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the privacy of Plaintiff's and Class's Sensitive Information, including duties imposed by the HIPAA, 45 C.F.R. § 160.102;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately protect Plaintiff's and Class's Sensitive Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the

security and privacy of Plaintiff's and Class's Sensitive Information, including duties imposed by HIPAA, 45 C.F.R. § 160.102 or the FTC Act, 15 U.S.C. § 45;

h. Omitting, suppressing, and concealing the material fact that it uses Pixel to share data and information with Meta, and extent of data sharing between visitors to North Memorial's Websites and Meta, in violation of both HIPAA, the FTC Act, and other common laws.

180. Defendant's acts and practices were "unfair" because they caused or were likely to cause substantial injury to patients which was not reasonably avoidable by patients themselves and not outweighed by countervailing benefits to patients or to competition.

181. The injury to patients from Defendant's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Sensitive Information.

182. Plaintiff and the Class could not have reasonably avoided injury because Defendant's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of patient healthcare decision-making and information gathering. By withholding important information from patients about the inadequacy of its privacy protections and Defendant's intentional use of Pixel on its website, Defendant created an asymmetry of information between it and patients that precluded patients from taking action to avoid or mitigate injury.

183. Defendant also engaged in "deceptive" acts and practices in violation of Minn. Stat. § 325D.44, including:

a. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have; and

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not.

184. Had Defendant disclosed to Plaintiff and the Class that it used Meta Pixel which publicly disclosed sensitive, medical information, Defendant would have been unable to continue this type of business practice and it would have been forced to adopt reasonable data privacy measures and comply with the law. Defendant was trusted with sensitive and valuable PII and PHI regarding millions of patients, including Plaintiff and the Class. Defendant accepted the responsibility of protecting the data while keeping the state of the tracking technologies used on its site and application secret from the public. Accordingly, Plaintiff and the Class acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

185. Defendant had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII and PHI in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between Defendant and Plaintiff and the Class as described herein. Defendant had exclusive or superior knowledge of the practices engaged in where private information related to health and safety was shared with third-parties which

Plaintiff and the members of the class had no reasonable manner of obtaining in advance, giving rise to a further duty to disclose.

186. As a direct and proximate result of Defendant's unfair, abusive, and deceptive acts or practices, Plaintiff and the Class have suffered and will continue to suffer injury and monetary damages, as described herein, including but not limited to; loss of value of their PII and PHI, and the deliberate violation of their privacy as alleged herein.

187. There is an ongoing and future harm to Plaintiff and the Class Members. An invasion of privacy can never be fully remedied through damages, as there is a loss of privacy and exposure of private facts that cannot be undone. Use of the Pixel also limits patients' abilities to use the North Memorial Websites without fear of the exposure of private and confidential medical information, thus limiting the ability to use those sites at all.

188. Plaintiff may return to North Memorial in the future for additional medical care, at which point she will be required or encouraged to use North Memorial's Websites.

189. If patients cannot trust that their sensitive private information will be kept private and secure, they may be less likely to seek medical treatment, which may lead to more serious health consequences. Additionally, maintaining confidentiality for health records is vitally necessary to maintaining public trust in the healthcare system as a whole.

190. Plaintiff and the Class seek all relief allowed by law, including injunctive relief, costs and attorneys' fees, and remedies cumulative.

COUNT V
Violation of the Minnesota Health Records Act Minn. Stat. §§ 144.291 and 144.293
(On Behalf of the Plaintiff and the Nationwide Class)

191. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

192. Under the Minnesota Health Records Act ("MHRA"), "health record" means any information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of a patient; the provision of healthcare to a patient; or the past, present, or future payment for the provision of healthcare to a patient. Minn. Stat. § 144.291, subd. 2(c).

193. The information Plaintiff and the Class members exchanged with Defendant on its website concerned the past, present, and future physical or mental health or condition and the provision of healthcare. Thus, that information constitutes "health records" as that term is defined in the MHRA.

194. Plaintiff and the Class members are "patients" at all relevant times as that term is defined under the MHRA. Minn. Stat. § 144.291, subd. 2(g).

195. Under the MHRA, it is unlawful for a third party to access a patient's health records from a provider, or a person who receives records from a provider, without the patient or the patient's legally authorized representative's consent, specific authorization in law, or a representative from a provider that holds a signed and dated consent from the patient authorizing the release. Minn. Stat. § 144.293, subd. 2(1-3).

196. Defendant's use of Meta Pixel resulted in Defendant providing a third party with Plaintiff's and the Class member's health records and, furthermore, allowed a

third party to access, without authorization, Plaintiff's and the Class members' health records.

197. Neither Plaintiff nor the Class members consented to or otherwise authorized Defendant to share their health records with Meta or any other third-party.

198. Under the MHRA, a provider or other person who causes an unauthorized release of a health record by negligently releasing the health record is liable to the patient for compensatory damages, plus costs and reasonable attorney fees. Minn. Stat. § 144.298, subd. 2. As a result of Defendant's violations of the MHRA, Plaintiff and the other Class members seek all damages authorized by law, including compensatory damages plus costs, and reasonable attorney fees.

COUNT VI
INVASION OF PRIVACY—INTRUSION UPON SECLUSION AND PUBLICATION OF PRIVATE FACTS
(On behalf of Plaintiff and Nationwide Class)

199. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

200. Plaintiff and the Class have an objective, reasonable expectation of privacy in their Website Communications and other online behaviors, particularly those containing sensitive medical information and those communicated via personal devices.

201. Plaintiff and the Class members did not consent to, authorize, or know about Defendant's intrusion of their privacy at the time it occurred. Plaintiff and the Class members never agreed that Defendant could embed Pixel to manipulate their website

sessions or disclose their Website Communications or other online behaviors gathered by Pixel, to its vendors and other third parties.

202. Plaintiff and the Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain. Plaintiff and the Class Members accessed Defendant's Websites from their personal devices, on which they automatically have an objective and reasonable expectation of privacy.

203. Additionally, Pixel secretly tracked Plaintiff and the Class Members' Website Communications and other online behaviors with a medical provider's website for the entire duration Plaintiff and the Class Members were on the Websites. Plaintiff and the Class Members had an objective and reasonable expectation of privacy in their medical related communications and communications containing Sensitive Information.

204. Through its privacy violations, Defendant secretly embedded Pixel to manipulate Plaintiff's website session and divulged Plaintiff's and the Class's highly private Sensitive Information to third parties, without prior consent or authorization. This disclosure is offensive to the reasonable person and Plaintiff's and the Class's medical or other private information are not matter of public concern.

205. Additionally, Defendant has intentionally intruded on Plaintiff's and the Class's private life, seclusion, or solitude, without consent. This conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

206. As a direct and proximate result of Defendant's unauthorized disclosure of Plaintiff's and the Class's private data and intrusion upon Plaintiff's seclusion, including embedding the Meta Pixel within the website browser and also the disclosure of intimately personal facts in the form of their Website Communications, Plaintiff and Class members suffered and continue to suffer harm and injury. Given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

207. Further, Defendant has improperly profited from its invasion of Plaintiff's and the Class members' privacy in its use of their data for its economic value.

208. Plaintiff and the Class members are entitled to damages, including compensatory, and/or nominal damages in an amount to be proven at trial.

209. To the extent Defendant's conduct is ongoing, and it continues to unlawfully disclose the communications of Plaintiff and the Class members any time they use or provide information to Defendant through its website or application without their consent, Plaintiff and the Class members are entitled to declaratory and injunctive relief. This will prevent future unlawful and unauthorized disclosure of Plaintiff's and the Class members' Sensitive Information.

COUNT VII
UNJUST ENRICHMENT
(On behalf of Plaintiff and the National Class)

210. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

211. Plaintiff and the Class members provided their Sensitive Information to Defendant for the purposes of receiving healthcare services or healthcare related information and knowledge. Defendant knowingly and unlawfully received a benefit from its use of Plaintiff's and the Class members' Sensitive Information, including monetary compensation. Defendant intentionally and knowingly collected and used Plaintiff's and the Class members' Sensitive Information for its own gain, without Plaintiff's or the Class Members' consent, authorization or compensation.

212. Defendant unjustly retained those benefits and enriched itself at the expense of Plaintiff and the Class members and this conduct damaged Plaintiff and the Class members. Plaintiff and the Class members were not compensated by Defendant for the data they unknowingly provided which holds intrinsic value.

213. It would be inequitable and unjust for Defendant to retain any of the profit or other financial benefits derived from the secret, unfair, and deceptive data tracking methods Defendant employes on northmemorial.com.

214. The Court should require Defendant to disgorge all unlawful or inequitable proceeds that it received into a common fund for the benefit of Plaintiff and the Class members, and order other such relief as the Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for judgment in her favor as follows:

a. Certification the Class pursuant to the provisions of Fed. R. Civ. P. 23 and an order that notice be provided to all Class Members;

b. Designation of Plaintiff as representative of the Class and the undersigned counsel as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. An order for injunctive relief, enjoining Defendant from engaging in the wrongful and unlawful acts described herein;

e. An award of statutory interest and penalties;

f. An award of costs and attorneys' fees; and

g. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully submitted,

Dated: June 27, 2023

s/ Brian C. Gudmundson

Brian C. Gudmundson (MN #336695)
Jason P. Johnston (MN #0391206)
Michael J. Laird (MN #398436)
Rachel K. Tack (MN #0399529)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Hart L. Robinovitch
ZIMMERMAN REED LLP
14646 N. Kierland Blvd., Suite 145
Scottsdale, AZ 85254
Telephone: (480) 348-6400
hart.robinovitch@zimmreed.com

Nathan D. Prosser (MN #0329745)
HELLMUTH & JOHNSON, PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 522-4291
nprosser@hjlawfirm.com

Attorneys for Plaintiff